UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

M

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,245	12/19/2000	Chin-Long Chen	POU920000088US1	4895

7590 08/18/2004

Lawrence D. Cutter, Attorney
IBM Corporation
Intellectual Property Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/740,245	**Applicant(s)** CHEN ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 May 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *5-17-2001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 12/19/2000.

Specification

3. The disclosure is objected to because of the following informalities: The Element 501 of Figure 17 is labeled as “NO REGISTER”. The proper label according to the specification should be N with the subscript zero (e.g., No REGISTER).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1 – 3 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to

make and/or use the invention. The issues and problems are addressed by each individual claim as follows.

5. As per claim 1, the following claim limitations are not enabled by the specifications: (a) Line 8: "for sequential values of i running from 0 to k-1, carrying out the following operations" – As understood by the examiner, the value of i should be running from 1 to k-1, (b) Line 9: "shifting the contents of the first storage element right by one bit position" – As understood by the examiner, the first storage element should be corrected to the second storage element, (c) Line 10: "determining the current rightmost bit in said first storage element" – As understood by the examiner, the first storage element should also be corrected to the second storage element, and (d) Line 12: "increasing the value stored in said second storage element by 2 and increasing the value stored in said first storage element by A" – As understood by the examiner, the entire claim limitation should be corrected to "increasing the value stored in said first storage element by 2 EXP(i) and increasing the value stored in said second storage element by A".

6. As per claim 2, the claim limitations are not enabled by the specifications due to the similar reasons as addressed above.

7. As per claim 3, the claim limitations are not enabled by the specifications according to the Figure 17. For example, Line 10 recites the limitation "an adder having as a first input the contents of said second register and a second input

from ...". According to the specification, the adder can't have as a first input the "exact" contents of said second register; otherwise, the enablement issues arise.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Arazi (Patent Number: 5448639), hereinafter referred to as Arazi.

9. As per claim1, Arazi teaches a method for calculating the multiplicative inverse of an odd binary number, A, modulo R, where R is positive integer power of two, 2 ^(k), said method comprising the steps of: (1) initializing a first storage element having k bits, for a variable S, to a binary 1, (2) initializing a second storage element having k bits, for a variable Q, with the number A whose multiplicative inverse modulo R is to be determined; for sequential values of i running from 0 to k - 1, carrying out the following operations: (a) shifting the contents of the first storage element right by one bit position; (b) determining the current rightmost bit in said first storage element; (c) upon said rightmost bit position being determined to be a 1, increasing the value stored in said second storage element by 2 and increasing the value stored in said first storage

element by A (Arazi, see for example, Figure 1, Column 1 Line 51 – 60 and Column 10 Line 60 – 67: Arazi teaches bit-level shift-subtracted operations to obtain modular multiplicative inverse including the ADDER, MUX, shift register and a FOR loop counter).

10. Claim 2 is rejected under 35 U.S.C. 102(e) as being anticipated by Koc (Patent Number: US 2002/0059353 A1), hereinafter referred to as Koc.

11. As per claim 2, Koc teaches a method for calculating the negative multiplicative inverse of an odd binary number, A, modulo R, where R is a positive integer power of two, 2^k, said method comprising the steps of: (1) initializing a first storage element having k bits, for a variable S, to a value of 2^(k- 1); (2) initializing a second storage element having k bits, for a variable Q, with the number A whose negative multiplicative inverse modulo R is to be determined; (3) for sequential values of i running from 0 to k - 1, carrying out the following operations: (a) shifting the contents of the first storage element right by one bit position; (b) determining the current rightmost bit in said first storage element; (c) upon said rightmost bit position being determined to be a 1, decreasing the value stored in said second storage element by 2^(i) and increasing the value stored in said first storage element by A (Koc, see for example, Paragraph [0063]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koc (Patent Number: US 2002/0059353 A1), hereinafter referred to as Koc.

13. As per claim 3, Koc teaches a method for calculating the negative a circuit for determining the negative multiplicative inverse of an odd binary number A, modulo R, where R is a positive power of two, 2^(k), said circuit comprising: (a) a first k bit register, for storing a variable S; (b) a second k bit register, for storing a variable Q; (c) a third k bit register, for storing said number A; (d) a counter capable of counting from 0 to k – 1; (e) a decoder receiving counter output from said counter; (f) means for setting bits from said decoder into said first register upon the condition that the next to rightmost bit in said second register is a one; (g) an adder having as a first input the contents of said second register, and a second input from said third register said second input being conditioned on the next to rightmost bit in said second register, with the output of said adder being supplied to said second register (Koc, see for example, Paragraph [0063]: Koc teaches a method to derive a negative of the multiplicative inverse with the module = 2 ^(k) (Koc, see for example, Paragraph

[0063]). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the algorithm into the logical circuitry because ADDER, MUX, shift register and a counter associated with FOR loop counter are all well known in the field).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Montgomery (Mathematics of Computation, Volume 44, Number 170, Pages 519 – 521, April 1985) discloses "Modular Multiplication Without Trial Division".

b. Shimbo (U.S. Patent Number US 6546104 B1) discloses "Montgomery Reduction Appratus".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100